CLAIMS

1. Authentication method for authenticating a mobile node to a packet data network, comprising the steps of:

providing the mobile node with a mobile node identity and a shared secret specific to the mobile node identity and usable by a telecommunications network;

providing the mobile node with a protection code;

sending the mobile node identity and the protection code from the mobile node to the packet data network;

providing the packet data network with authentication information usable by the telecommunications network, the authentication information comprising a challenge and a session secret corresponding to the mobile node identity and derivable using the challenge and the shared secret;

forming cryptographic information using at least the protection code and the session secret;

sending the challenge and the cryptographic information from the packet data network to the mobile node;

checking at the mobile node the validity of the cryptographic information using the challenge and the shared secret;

generating at the mobile node the session secret and a first response corresponding to the challenge, based on the shared secret;

sending the first response to the packet data network; and

checking the first response for authenticating the mobile node.

2. Method according to claim 1 further comprising the steps of:

providing the mobile node with a subscriber identity for the telecommunications network; and

forming from the subscriber identity a Network Access Identifier as the mobile node identity by the mobile node.

3. Method according to claim 1 further comprising the step of recognising the telecommunications network at the packet data network directly from the mobile node identity.

4. Method according to claim 1, further comprising the step of providing the packet data network with a shared session key based on the at least one

session secret.

5. Method according to claim 1, further comprising the step of providing a communications link between the packet data network and the mobile node for communicating the challenge between them, the communications link not being a link of the telecommunications network.

6. Method according to claim 1, further comprising the step of using a Subscriber Identity Module for the providing the mobile node with a mobile node identity and the generating of the session secret based on a shared secret specific for the mobile node identity.

7. Method according to claim 6, wherein the step of providing the mobile node with the mobile node identity and the shared secret specific for the mobile node identity further comprises the sub-steps of:

forming a local connection between the mobile node and a subscriber identity module; and

receiving from the subscriber identity module to the mobile node the mobile node identity and a session secret specific to the mobile node identity.

8. Method according to claim 1, further comprising the steps of:

obtaining a second response by the telecommunications network; and

using the second response in the checking the first response.

9. Method according to claim 1, further comprising the step of sending the challenge is sent from the telecommunications network to the mobile node via the packet data network.

10. Method according to claim 1, wherein the protection code is based on time.

11. Method according to claim 1, wherein the challenge is based on RAND codes of at least two authentication triplets of the telecommunications network.

12. Method according to claim 1, further comprising the step of generating a shared session key for Internet Key Exchange, wherein the shared session key is based on the at least one session secret and the at least one challenge.

13. Authentication method in a mobile node for authenticating a mobile node to a packet data network, comprising the steps of:

providing the mobile node with a mobile node identity and a shared secret specific to the mobile node identity and usable by a telecommunications network;

providing the mobile node with a protection code;

sending the mobile node identity and the protection code to the packet data network;

receiving a challenge and cryptographic information from the packet data network;

checking the validity of the cryptographic information using the challenge and the shared secret;

generating a session secret and a first response corresponding to the challenge, based on the shared secret; and

sending the first response to the packet data network.

14. Method for communicating between a packet data network and a mobile node having an access to a subscriber identity of a mobile telecommunication network, comprising the steps of:

providing a mobile node with a subscriber identity for the telecommunications network; and

forming, by the mobile node, of the subscriber identity a Network Access Identifier as a mobile node identity for use by the packet data network.

15. Gateway for acting as an interface between interfacing a packet data network and a telecommunications network having an access to an authentication server, the gateway comprising:

an input for receiving a mobile node identity and a protection code from the packet data network;

an output for providing the authentication server with the mobile node identity;

an input for receiving a challenge and a session secret corresponding to the mobile node identity from the authentication server;

a first processor for forming cryptographic information using at least the protection code and the session secret;

an output for providing the packet data network with the challenge and the cryptographic information for further transmission to a mobile node;

an input for receiving a first response corresponding to the challenge, based on a shared secret specific to the subscriber identity and known by the mobile node and the telecommunications network, from the mobile node via the packet data network; and

a second processor for verifying the first response for authenticating the mobile node.

16. Gateway for acting as an interface between a packet data network and a telecommunications network having an access to an authentication server, the gateway comprising:

a first input for receiving a Network Access Identifier from the packet data network;

a processor for forming a subscriber identity suitable for use in the telecommunications network from the Network Access Identifier;

a first output for providing the telecommunications network with the subscriber identity;

a first input for receiving from the authentication server a challenge and a session secret corresponding to the challenge and to the subscriber identity; and

a second output for providing the packet data network with the challenge.

17. Communication system comprising:

a telecommunications network;

a packet data network comprising;

a mobile node comprising a first processor for forming a protection code;

a gateway for acting as an interface between the packet data network with the telecommunications network;

a subscriber identity module accessible by the mobile node comprising a subscriber identity and a shared secret;

an authentication server for the telecommunications network comprising the shared secret mapped to the subscriber identity;

the authentication server being adapted to receive the subscriber identity and responsively to return a challenge;

the gateway comprising a second processor for forming cryptographic information based on the protection code;

the mobile node being adapted to receive from the gateway the challenge and the cryptographic information; and being adapted to provide the subscriber identity module with the challenge to responsively to receive a first response based on the challenge and the shared secret;

the first processor being further adapted to verify the protection code to

authenticate the gateway to the mobile node; and

a third processor accessible by the gateway for verifying the first response in order to authenticate the mobile node.

18. Communication system comprising:

a telecommunications network;

a packet data network;

a mobile node having a mobile node identity;

a gateway for acting as an interface between the packet data network with the telecommunications network;

a subscriber identity module accessible by the mobile node comprising a subscriber identity and a shared secret;

an authentication server for the telecommunications network comprising the shared secret mapped to the subscriber identity;

a first processor accessible by the gateway for forming the subscriber identity of the mobile node identity for the telecommunications network;

the authentication server being adapted to receive the subscriber identity and responsively to return a challenge;

the subscriber identity module being adapted to receive the challenge and responsively to form a first response based on the challenge and the shared secret; and

a second processor accessible by the gateway for verifying the first response in order to authenticate the mobile node.

19. Mobile node comprising:

a Subscriber Identity Module having a subscriber identity for identifying the subscriber to a telecommunication network and a shared secret specific to the subscriber identity module and known by an authentication server accessible by the telecommunication network;

a processor for forming a mobile node identity based on the subscriber identity; and

a communication block for communicating with a packet data network, adapted to send the mobile node identity to the packet data network and to receive in response a challenge from the packet data network;

wherein the subscriber identity module is adapted to form a first response

corresponding to the challenge, based on the shared secret.

20. Computer program product for controlling a mobile node for authenticating the mobile node to a packet data network, comprising:

computer executable code to enable the mobile node to obtain a mobile node identity and a shared secret specific to the mobile node identity and usable by a telecommunications network;

computer executable code to enable the mobile node to obtain a protection code;

computer executable code to enable the mobile node to send the mobile node identity and the protection code to the packet data network;

computer executable code to enable the mobile node to receive a challenge and cryptographic information from the packet data network;

computer executable code to enable the mobile node to check the validity of the cryptographic information using the challenge and the shared secret;

computer executable code to enable the mobile node to generate a session secret and a first response corresponding to the challenge, based on the shared secret; and

computer executable code to enable the mobile node to send the first response to the packet data network.

21. Computer program product for controlling a mobile node to communicate with a packet data network, mobile node having an access to a subscriber identity usable by a telecommunications network, the computer program product comprising:

computer executable code to enable the mobile node to provide a mobile node with the subscriber identity; and

computer executable code to enable the mobile node to form a Network Access Identifier of the subscriber identity as a mobile node identity for use by the packet data network.

22. Memory medium containing a computer program product according to claim 20.